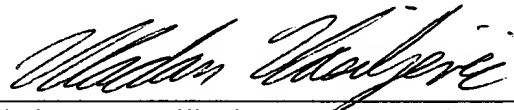
REMARKS

The changes to the specification only seek to correct typographical errors in the application.

Conclusion

If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,



Vladan M. Vasiljevic, Reg. No. 45,177
One of the Attorneys for Applicant(s)
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: March 5, 2003

PATENT
Attorney Docket No. 205724

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Moore et al.
Application No. 09/694,514

Group Art Unit: 2132
Examiner: Unassigned

Filed: October 23, 2000

For: SECURITY LINK MANAGEMENT IN DYNAMIC NETWORKS

AMENDMENT TO THE SPECIFICATION AS OF March 5, 2003

A replacement page for page 16 of the application, showing typographical corrections, follows the current sheet.

administrator verifies the identity of the user, i.e., authenticate the user, then the domain controller permits the user to logon in step 830. The domain controller then obtains a certificate to prove the user's identity during step 835. At step 840 subsequent access to the computing resources utilizes the certificate to prove the user's identity without the need to invoke the system administrator.

FIGURE 9 illustrates an exemplary method for providing limited access to a user in a remote and non-secure site, which may be defined as requiring the use of one or more machines whose identity is unknown or a physical location that is outside of the intranet. In such a scenario it is advantageous to provide limited access that does not reflect all of the privileges the particular user may have had if operating from a secure site or machine. In step 900 a request for access is made to a remote access point at via a proxy server followed by the customary request for an assertion of an identity in step 905. Providing an identity, which may be a user or machine identity, during step 910 results in a challenge during step 915 to prove the asserted identity. Step 920 includes the requester proving the asserted identity by providing a certificate from a trusted certificate authority. The radius proxy server forwards the relevant transactions and the radius server charged with policing the security provides a Universal Resource Locator ("URL") to the user, in effect a port address, to allow access to the computing environment at step 925. This URL typically provides a lesser degree of access to network resources by the user than the user would receive via an access point in the network.

FIGURE 10 summarizes steps in another embodiment of the invention for remote access to a secure computing resource. Step 1000 includes a request by a remote user to access a resource in a secure computing environment. This request may be made at an access point in another network and over the Internet. A RADIUS server handles the request and provides a URL in step 1005 to permit the requester to authenticate at the distant site. This connection is likely to be a secure connection, as is indicated in step 1010, and may use SSL and other similar technologies to authenticate the requester. In addition, the web page used for authentication may also request and accept information for accounting purposes. Such information includes credit card numbers, the time and nature of resources requested and the like. At step 1015 a determination is made if the requested services are available. If the services are available an the authentication is